La logique des parties fractionnaires de nombres réels

Luc BÉLAIR [a], Françoise POINT [b]

[a] *Département de mathématiques, Université du Québec, C.P. 8888, succ. Centre-ville, Montréal, Québec, H3C 3P8*
[b] *Département de mathématiques, Université de Mons, Le Pentagone, 20, Place du Parc, B-7000 Mons, Belgique*

Reçu le *****; accepté après révision le +++++

Présenté par ČČČČČ

Résumé

Le groupe des décimales avec l'addition modulo 1 et l'ordre naturel, qui n'est pas un groupe ordonné au sens habituel, est utilisé pour améliorer l'efficacité des automates temporels ([1]). Dans cette note, on donne une axiomatisation de cette structure, et on montre qu'elle admet l'élimination des quantificateurs.

Abstract

The logic of fractional parts of real numbers. The group of decimals with addition modulo 1 and the natural order, which is not an ordered group in the usual sense, is used to enhance the efficiency of timed automata ([1]). In this note, we axiomatize this structure and show it admits quantifier elimination.

1. Introduction

Pour améliorer l'efficacité des automates temporels, Bouchy-Finkel-Leroux [1] ont considéré la possibilité de représenter un ensemble de vecteurs réels en parties entières et parties décimales. Ainsi, ils montrent qu'un ensemble définissable dans la structure $(\mathbb{R}, \mathbb{Z}, +, <)$ se décompose en une réunion finie d'ensembles de la forme $Z + D$ tel que Z est un ensemble définissable dans la structure $(\mathbb{Z}, +, <)$ et D est un ensemble définissable dans la structure $([0, 1[, +_1, <)$, où $+_1$ désigne l'addition modulo 1. On sait que la théorie de la structure $(\mathbb{R}, \mathbb{Z}, +, <)$ est décidable (voir [1]) et Weispfenning ([7]) a montré qu'elle admet l'élimination des quantificateurs en ajoutant les constantes $0, 1$, la fonction partie entière, et les relations de congruence modulo chaque entier naturel positif. La théorie du premier ordre de la structure $(\mathbb{Z}, +, <)$ est l'arithmétique de Presburger, et la théorie de la structure $(\mathbb{R}, +, <)$ est celle des groupes abéliens ordonnés divisibles. Il semble naturel de vouloir compléter le portrait dressé par Bouchy et al.

Email addresses: belair.luc@uqam.ca (Luc BÉLAIR), point@math.univ-paris-diderot.fr; Directeur de recherches au FRS-FNRS (Françoise POINT).

en s'arrêtant de plus près sur la théorie du premier ordre de la structure $([0,1[,+_1,<)$. On sait qu'elle est décidable, puisque interprétable dans $(\mathbb{R},+,<)$. Dans cette note, nous en donnons une axiomatisation et montrons qu'elle admet l'élimination des quantificateurs. Cette structure a plutôt été considérée dans la littérature comme un *groupe cycliquement ordonné*, à savoir le groupe du cercle unité $(S^1,\cdot)$ avec l'ordre circulaire induit c'est-à-dire la relation ternaire $R(X,Y,Z)$ affirmant que les points X,Y,Z apparaissent dans cet ordre quand on enroule l'intervalle $[0,1[$ sur le cercle par la fonction exponentielle $t \mapsto e^{2\pi it}$. Une axiomatisation de la structure $(S^1,\cdot,R)$ a été donnée par Lucas dans sa thèse (voir [6], [5], [3]), et cette théorie admet aussi l'élimination des quantificateurs. Nous relions les deux points de vue à la fin de cette Note. Pour nos résultats, nos méthodes « à la main » sont plus directes que [3] (où est utilisé l'enroulement de $\mathbb{R}$ entier), et plus dans l'optique de [1]. Dans un article plus détaillé, nous traiterons le cas plus général des structures $(G \cap [0,1[,+_1,-_1,0,<)$ où G est un sous-groupe dense quelconque de $(\mathbb{R},+)$. On pose $\mathbb{N}^* = \mathbb{N}\setminus\{0\}$. On utilise le caractère gras $\mathbf{x}$ pour désigner un uplet, avec parfois des abus de notation correspondants. Rappelons qu'une sous-structure H d'une structure K y est dite existentiellement close, noté $H \subseteq_{ec} K$, si pour toute formule sans quantificateur $\varphi(\mathbf{x})$ de la logique du premier ordre formulée en termes des opérations et relations de base de H et K et de paramètres dans H, on a que $\varphi(\mathbf{x})$ possède une solution dans H ssi elle en possède une dans K. Un exemple est fourni par une extension de groupe abélien ordonné divisible $H \subset K$. Une théorie du premier ordre est modèle-complète si pour tout modèle H qui est une sous-structure d'un autre modèle K, on a automatiquement $H \subseteq_{ec} K$. Un exemple est fourni par la théorie des groupes abéliens ordonnés divisibles.

2. Le groupe des décimales avec son ordre naturel

Soit $[0,1[= \{r \in \mathbb{R} : 0 \leq r < 1\}$. L'addition modulo 1, notée $+_1$, en fait un groupe abélien isomorphe à $\mathbb{R}/\mathbb{Z}$. On considère aussi l'ordre naturel induit de $\mathbb{R}$. On obtient la structure $\mathbb{D} := ([0,1[,+_1,-_1,0,<)$. Ce n'est pas un *groupe ordonné* au sens habituel, par ex. $\mathbb{D}$ n'est pas sans torsion. Nous axiomatisons la théorie du premier ordre de $\mathbb{D}$ et montrons l'élimination des quantificateurs (§.4). La preuve utilise la possibilité de décomposer les modèles suffisamment saturés en un produit direct d'une partie « finie »(isomorphe à $\mathbb{D}$) et d'une partie « infinitésimale »(lemmes 3.4 et 4.1). L'élément $\frac{1}{2}$ est définissable dans $\mathbb{D}$ par la formule $y \neq 0$ & $2y = 0$. De même, pour $n > 2$, les éléments $\frac{1}{n}$ sont définissables sans quantificateur : $\frac{1}{n}$ est l'unique z tel que $nz = 0$ & $\wedge_{1\leq j\leq n-1}\, z < jz$. Pour chaque entier naturel $n, n \neq 0,1$, on considère la fonction $f_n : \mathbb{D} \to \mathbb{D}$ définie par $f_n(x) :=$ le plus petit y tel que $ny = x$, i.e $f_n(x) = \frac{x}{n}$. Notons que dans $\mathbb{D}$ on a $f_n(x) = z \leftrightarrow (nz = x$ & $\bigwedge_{0\leq i\leq n-1} z \leq z + \frac{i}{n})$.

La difficulté pour axiomatiser $\mathbb{D}$ réside dans les propriétés qui font interagir la structure de groupe et l'ordre. Le lien se fait par la fonction $-_1$ et la torsion. L'usage des f_n et $\frac{i}{n}$ est plus commode pour formuler nos axiomes et d'un point de vue technique.

Définition 2.1 *Soit le langage du premier ordre $L = \{+,-,0,<\}$, correspondant à la situation ci-dessus. Soit le langage du premier ordre $\mathcal{L}$ obtenu de L en ajoutant le symbole de constante $\frac{1}{2}$ et les symboles de fonctions unaires $f_n, n \in \mathbb{N}, n \neq 0,1$. Dans $\mathcal{L}$ on utilisera $\frac{i}{n}$ pour désigner le terme $2if_n(\frac{1}{2}), n \in \mathbb{N}, n \neq 0,1,2, 0 < i \leq n-1$.*

Soit $\mathcal{T}$ la théorie du langage $\mathcal{L}$ formée des axiomes suivants :

(1) les axiomes de groupe abélien ;

(2) la relation $<$ est un ordre strict total où 0 est le minimum ;

(3) $\forall x \forall y[(x < y \to (x < x + f_2(y-x) < y)) \& (x \neq 0 \to x < x + f_2(-x))]$;

(4) $\forall x \forall y (x < y \to -y < -x)$;

(5) $\forall x \left(\frac{1}{2} \neq 0 \;\&\; 2\frac{1}{2} = 0 \;\&\; (2x = 0 \to (x = 0 \vee x = \frac{1}{2}))\right)$;

Les trois axiomes suivants pour chaque entier naturel $n \neq 0, 1$.

(6) $\forall x \forall y\ (nf_n(x) = x\ \&f_n(x) \leq x\ \&\ (ny = x \to f_n(x) \leq y))$;

(7) $\forall x \left(\bigwedge_{0\leq i<n-1}(\frac{i}{n} \neq 0\ \&\ n\frac{i}{n} = 0)\ \&\ \left(nx = 0 \to \bigvee_{0\leq i<n-1} x = \frac{i}{n}\right)\right)$;

(8) $\frac{1}{n} < \frac{2}{n} < \ldots < \frac{n-1}{n}$.

(9) Pour tous les entiers naturels $m, n, m\prime, n\prime \neq 0, 1$, l'axiome suivant :

$$\bigwedge_{i,j,i\prime,j\prime,0<\frac{i}{n}+\frac{j}{m}<1} \left((\frac{i\prime}{n\prime} \leq x \leq \frac{i}{n}\ \&\ \frac{j\prime}{m\prime} \leq y \leq \frac{j}{m}) \longrightarrow \frac{i\prime}{n\prime} + \frac{j\prime}{m\prime} \leq x + y \leq \frac{i}{n} + \frac{j}{m}\right)$$

où $0 \leq i\prime < n\prime, 0 \leq i < n, 0 \leq j\prime < m\prime, 0 \leq j < m$ et $\frac{0}{k} := 0$.

(10) Pour chaque entier naturel $n \geq 3$, l'axiome suivant :

$$(x \leq \frac{1}{n}\ \&\ y \leq \frac{1}{n}\ \&\ z \leq \frac{1}{n}) \to ((x \leq y \leftrightarrow x + z \leq y + z)\ \&\ (x \leq x + y))\,.$$

Les axiomes cruciaux (8)-(9)-(10) donnent des relations entre l'addition, la torsion et l'ordre. On vérifie directement que $\mathbb{D}$ est un modèle de $\mathcal{T}$. On remarque que $\mathcal{T}$ est une théorie universelle.

Définition 2.2 *Soit T la théorie du langage L obtenue de $\mathcal{T}$ en remplaçant chaque occurence de $\frac{1}{2}$ par une nouvelle variable, disons u, et en insérant la condition supplémentaire $\exists u(u \neq 0 \& 2u = 0)$, et en remplaçant chaque occurence de $f_n(t)$ par une nouvelle variable, disons v, et en insérant la condition supplémentaire $\exists v(nv = t \& \forall v\prime(nv\prime = t \to v \leq v\prime))$.*

Par exemple, $x = \frac{1}{2}$ devient $\exists u(u \neq 0 \& 2u = 0 \& x = u)$, $f_2(y - x) < y$ devient $\exists v(2v = y - x \& \forall v\prime(2v\prime = y - x \to v \leq v\prime) \& v < y)$, et $2f_n(\frac{1}{2}) < x$ devient $\exists u \exists v(u \neq 0 \& 2u = 0 \& nv = u \& \forall v\prime(nv\prime = u \to v \leq v\prime) \& 2v < x)$.

On vérifie directement que tout modèle de $\mathcal{T}$ donne naturellement un modèle de T et vice versa.

Lemme 2.3 *Les propriétés suivantes sont des conséquences de $\mathcal{T}$.*

a) $-\frac{i}{n} = \frac{n-i}{n}$, $\frac{1}{n} = \frac{m}{nm}$, *et* $\frac{i}{n} \leq \frac{j}{m}$, *si* $im \leq jn$.

b) $x < -x \leftrightarrow x < \frac{1}{2}$ *et* $(x < -x\ \&\ -y < y) \to x < y$.

c) $f_n(x) = z \leftrightarrow (nz = x\ \&\ \bigwedge_{0\leq i\leq n-1} z \leq z + \frac{i}{n})$.

Définition 2.4 Soit H un modèle de T, on pose $H^{00}_+ = \{x \in H : x < \frac{1}{n}, \forall n \in \mathbb{N}, n \geq 2\}$ (ce sont les « infiniment petits » de H), $H^{00}_- = \{x \in H : -x < \frac{1}{n}, \forall n \in \mathbb{N}, n \geq 2\}$, et $H^{00} = H^{00}_+ \cup H^{00}_-$.

Lemme 2.5 *Soit H un modèle de T, et $a, b \in H$ tels que $a, b \in H^{00}_+$ et $a < b$, alors $b - a \in H^{00}_+$.*

Notons que H^{00}_+ et H^{00}_- sont définissables sans quantificateurs dans H^{00} : $x \in H^{00}_+ \leftrightarrow x \in H^{00} \& (x < -x \vee x = 0)$, $x \in H^{00}_- \leftrightarrow x \in H^{00} \& (-x < x \vee x = 0)$.

Lemme 2.6 *Soit H un modèle de T. Alors H^{00} est un sous-groupe pur divisible de H et sans torsion.*

Preuve. Par définition on a $0 \in H^{00}_+, x \in H^{00}_+ \to -x \in H^{00}_-, x \in H^{00}_- \to -x \in H^{00}_+$. L'ensemble H^{00}_+ est clos pour $+$ par l'axiome (9), et alors H^{00}_- aussi en passant par la fonction $-$. Soit $x \in H^{00}_+, y \in H^{00}_-$, non nuls, et considérons $x + y$. Si $x = -y$, alors $x + y = 0$. Si $x > -y$, alors $x - (-y) = x + y \in H^{00}_+$ par le lemme 2.5. Si $x < -y$, alors $-y - x \in H^{00}_+$ par le lemme 2.5, d'où $x + y \in H^{00}_-$. Ainsi H^{00} est un sous-groupe. Il est sans torsion par l'axiome (7). Il est pur par l'axiome (9). □

Remarquons que, avec l'ordre induit, H^{00} n'est pas un groupe abélien ordonné au sens habituel, à moins d'être trivial, puisque 0 y est un minimum. Cependant, H^{00}_+ est la partie positive d'un unique groupe abélien ordonné. Cela découle de résultats bien connus (voir [2]), que nous esquissons dans §.3.

3. Les monoïdes commutatifs ordonnés

Définition 3.1 *Soit L_{mo} le langage $\{+, 0, <\}$, et soit T_{mo} la théorie de ce langage formée des axiomes suivants : les axiomes de monoïde commutatif, la relation $<$ est un ordre total, $\forall a \forall b \forall c\ (a + c \leq b + c \leftrightarrow a \leq b)$. Soit T_{mon} la théorie obtenue de T_{mo} en ajoutant les deux axiomes suivants : $\forall a \forall b (a \leq a + b)$, $\forall a \forall b\ (a < b \rightarrow \exists c(a + c = b))$. Finalement, soit T_{md} la théorie obtenue de T_{mon} en ajoutant les axiomes de divisibilité $\forall a \exists b(nb = a), n \in \mathbb{N}, n \geq 2$.*

On vérifie que si H est un modèle de $\mathcal{T}$, alors H^{00}_+ et H^{00}_- sont des modèles de T_{mon}. Puisque $f_n(x) \leq x$ (axiome (6)), on a aussi que H^{00}_+ est un modèle de T_{md} .

On sait que tout modèle S de T_{mo} se plonge dans un groupe abélien totalement ordonné G, unique à isomorphisme près, tel que tout élément de G est la différence de deux éléments de S (voir par exemple [2], théorème 2). De plus, on a alors que $S = \{g \in G : g \geq 0\}$ si et seulement si S est un modèle de T_{mon}. Le fait que la théorie des groupes abéliens totalement ordonnés divisibles soit modèle-complète dans L_{mo} entraîne alors que la théorie T_{md} du langage L_{mo} est modèle-complète.

Définition 3.2 Soit $T_{d,<}$ la théorie du langage L obtenue de la théorie des groupes abéliens sans torsion, en ajoutant les axiomes suivants : la relation $<$ est un ordre strict total, la fonction $x \mapsto -x$ renverse l'ordre, l'ensemble $\{x : x < -x\} \cup \{0\}$ est un modèle de T_{md}, et finalement $((x < -x\ \&\ -y < y) \rightarrow x < y)$.

Les modèles de $T_{d,<}$ sont divisibles, puisque si $x \neq 0$, on a soit $x < -x$, soit $-x < x = -(-x)$, d'où x ou $-x$ divisible par n (par T_{md}), et donc x divisible par n, pour tout entier n. Notons que $H^{00} \models T_{d,<}$. Pour montrer la proposition suivante, on montre d'abord que $T_{d,<}$ est modèle-complète, par réduction à T_{md}. Puis, en notant que pour toute sous-structure A dans un modèle F sa clôture divisible $\tilde{A}$ dans F est aussi un modèle, on montre que $\tilde{A}$ se plonge au-dessus de A dans tout autre modèle contenant A.

Proposition 3.3 *La théorie $T_{d,<}$ admet l'élimination des quantificateurs dans le langage L.*

Soit H un modèle de T, on note H_{tor} son sous-groupe de torsion. On a $H_{tor} = \{\frac{i}{n} : n, i \in \mathbb{N}, n \neq 0, 1, 0 \leq i < n\}$. Pour $g \in H$, on définit sa *coupure* dans H_{tor}, à savoir le couple d'ensembles $C^-(g) := \{h \in H_{tor} :\ h < g\}$, $C^+(g) := \{h \in H_{tor} :\ g < h\}$. On remarque que $C^+(g) = \emptyset \leftrightarrow g \in H^{00}_-$ et $C^-(g) = \emptyset \leftrightarrow g \in H^{00}_+$. On obtient le lemme suivant, en prenant *la partie standard* obtenue à l'aide des *coupures* ci-dessus. Rappelons qu'un modèle $\aleph_1$-saturé de T est un modèle tel que tout ensemble dénombrable de formules à paramètres, qui est finiment satisfaisable, est automatiquement satisfaisable. Ainsi, un modèle $\aleph_1$-saturé de T possède assurément des infiniment petits non nuls.

Lemme 3.4 *Supposons H un modèle de T qui soit $\aleph_1$-saturé. Alors H^{00} est un facteur direct de H et $(H/H^{00}, +, 0) \cong ([0, 1[, +_1, 0)$.*

4. Élimination des quantificateurs et complétude

Dans le lemme suivant, l'argument clé avec les projections provenant du lemme 3.4, s'apparente à [4].

Lemme 4.1 *Soit H, K des modèles $\aleph_1$-saturés de $\mathcal{T}$ tel que $H \subseteq K$. Alors $H \subseteq_{ec} K$.*

Il découle directement de ce lemme que la théorie $\mathcal{T}$ est modèle-complète dans le langage $\mathcal{L}$. On obtient aussi T modèle-complète, car $\mathcal{T}$ l'est et f_n est définissable existentiellement dans L à partir des $\frac{i}{n}$.

Posons $\mathbb{D}_{\mathbb{Q}} = (\mathbb{Q} \cap [0, 1[, +_1, -_1, 0, <)$. On vérifie directement que $\mathbb{D}_{\mathbb{Q}} \models \mathcal{T}$ et que si $H \models \mathcal{T}$ alors $\mathbb{D}_{\mathbb{Q}} \subseteq H$ par l'identification naturelle avec les $\frac{i}{n}$. Il s'ensuit que $\mathcal{T}$, étant modèle-complète, est aussi complète et décidable. La théorie $\mathcal{T}$ a une axiomatisation universelle et est modèle-complète, elle admet donc l'élimination des quantificateurs dans $\mathcal{L}$. Ainsi, la théorie $\mathcal{T}$ (ou T) axiomatise $\mathbb{D}$. On peut aussi montrer que T élimine les quantificateurs dans L. Il s'agit en quelque sorte d'éliminer les f_n et $\frac{i}{n}$.

On peut faire le lien suivant avec le point de vue des groupes cycliquement ordonnés. Soit $R_{\mathbb{D}}$ la relation ternaire sur $[0, 1[$ définie par $R_{\mathbb{D}}(x, y, z) \leftrightarrow x < y < z \vee y < z < x \vee z < x < y$, et posons

$\mathbb{D}_c = ([0,1[, +_1, 0, R_{\mathbb{D}})$. Pour tous $x, y \in [0,1[$, on a $x < y \leftrightarrow R_{\mathbb{D}}(0,x,y)$. On vérifie directement que $\mathbb{D}_c$ est un groupe cycliquement ordonné. Soit T_c l'axiomatisation de Lucas de la théorie du premier ordre de $\mathbb{D}_c$. Avec ces traductions, il suit des remarques précédentes que les axiomes de T se déduisent de T_c et vice versa. En particulier, certaines propriétés se transfèrent d'une théorie à l'autre. Par exemple, l'élimination des quantificateurs, le fait de ne pas avoir la propriété d'indépendance, etc. .

Remerciements

Soutien CRSNG Canada. Les auteurs remercient respectivement le groupe de logique du département de mathématiques de l'université Berkeley et le MSRI, pour leur hospitalité au cours du premier semestre 2014. Dédié à la mémoire de Jacqueline Charbonneau-Bélair.

Références

[1] F. Bouchy F., A. Finkel et J. Leroux, *Decomposition of Decidable First-Order Logics over Integers and Reals*, in Temporal Representation and reasoning, Proceedings of the 15th Symposium TIME 2008, IEEE Computer Society Press, 2008, pp. 147–155.

[2] A. Clifford, *Totally ordered commutative semigroups*, Bull. Amer. Math. Soc. **64** (1958) 305–316.

[3] M. Giraudet, G. Leloup et F. Lucas, First-order theory of cyclically ordered groups, arXiv :13-11.0499, 2013.

[4] S. Ibuka S., H. Kikyo et H. Tanaka, *Quantifier Elimination for Lexicographic Products of Ordered Abelian Groups*, Tsukuba J. Math. **33** (2009), 95–129.

[5] G. Leloup, *Autour des groupes cycliquement ordonnés*, Ann. Fac. Sci. Toulouse – Math. **XXI** (2012) 235-257.

[6] F. Lucas, *Théorie des modèles des groupes cycliquement ordonnés divisibles*, in Séminaire de structures algébriques ordonnés, Prépublications de l'Université Paris VII, no 56, 1996.

[7] W. Weispfenning, *Mixed Real-Integer Linear Quantifier Elimination*, in Symbolic and Algebraic Computation, Proceedings ISSAC'99, Vancouver BC, ACM, 1999, pp. 129–136.